United States District Court

District of Massachusetts

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Criminal No. 08CR10318-NG
STEVEN WATT,	)	
	)	
Defendant	)	

GOVERNMENT'S SENTENCING MEMORANDUM

Steven Watt ("Watt") designed, refined and provided the key computer hacking program in the largest identify theft in our Nation's history. Collaborating with Albert Gonzalez ("Gonzalez"), who had gained access to the computers processing credit and debit card transactions for TJX Companies, Inc. and its subsidiaries, Watt engineered software needed by his co-conspirators to collect tens of millions of victims' payment card numbers as their purchases in stores were being processed.

The principal contested issue before the Court at sentencing will be whether or not Watt knew he was collaborating in an effort to break into the computer networks of major businesses and to steal from them the credit and debit card numbers of vast numbers of victims. As the facts set out in the next few pages will demonstrate, it is beyond cavil that Watt worked closely with Gonzalez on electronic intrusions of major businesses, knew the purpose of these intrusions was massive and widely publicized

identify theft, and knew that the conspirators were profiting handsomely from their scheme.

Background

Neither the most basic facts, nor the conclusions to be drawn from them, are in dispute. Albert Gonzalez led a group which, between approximately 2004 and 2007, hacked into the computer systems processing credit and debit card transactions for a number of major retailers. Once in those systems, the group sought to locate where customers' credit numbers, debit card numbers and PINs were stored, or where they could be electronically captured as transactions were being processed. The group then stole tens of millions of credit and debit card numbers from retailers, selling vast numbers here and abroad for fraudulent use, and obtaining hundreds of thousands of dollars of cash advances fraudulently in the United States at ATMs using the stolen identities. The retailer which suffered the greatest loss at the hands of the group was TJX Companies. After breaking into TJX's financial transaction processing computers in Framingham, Massachusetts, the group initially found and stole a number of card numbers which had been in storage. Finding many of these to be old or expired, the group then sought to capture credit card numbers and debit card numbers in the system as transactions were being processed among TJX's stores and subsidiaries.

In order to capture ongoing transactions, however, the group needed what is colloquially known as a "sniffer" program. "Sniffer" programs monitor traffic as it goes across a computer network and can be used for legitimate purposes, or, as here, for malicious ones. In this instance, Watt specifically configured a "sniffer" program for the group to monitor that portion of the network's traffic that contained the payment card numbers being processed. As a consequence of the intrusion and data theft, TJX has suffered approximately two hundred million dollars in damages, as detailed in its most recent, 2009 SEC 10-K filing.

Watt and Gonzalez were extremely close friends, communicating sometimes several times a day, both over the phone and through extended instant message conversations. Agents have recovered approximately 300 pages of logged exchanges of instant messages between Watt and Gonzalez from one of Gonzalez's laptop computers. The exchanges took place over the course of approximately a year immediately prior to Watt's collaboration with Gonzalez in the TJX data theft in May, 2006, and provide an intimate look at just how closely they shared all of their exploits: sexual, narcotic and hacking. The exchanges demonstrate Watt's clear knowledge of the immensity of the scheme to steal and abuse credit card numbers and debit card numbers, and his intent to support the scheme by providing specifically configured malicious software when asked.

Watt Knowingly and Repeatedly Assisted Gonzalez in His Efforts to Compromise Major Computer Networks

The logged instant messenger communications between Gonzalez and Watt reflect that the two were already working together by March and April, 2005, to gain and maintain unauthorized access into large corporate and educational networks. As he would later with TJX, Gonzalez asked Watt to write malicious software (code) designed to capture without detection valuable information being utilized by the networks (in this case user names and passwords). Their continuing collaboration is exemplified during this period by their shared efforts to gain unauthorized access first to bizrate.com's network, then to fortunecity.com's, and finally Florida International University's network.

On March 9, 2005, Watt reported that he was unsuccessful in his attempt to log onto a computer system at bizrate.com and checked with Gonzalez to see if he was using the correct credentials. Gonzalez provided the user name "rsabuber" to try. Watt reported back that bizrate.com did not utilize user names/passwords but rather secure key pairs for authentication to the system. He then, in turn, sent Gonzalez an RSA private key and told Gonzalez to save it.

A few weeks later on April 1, 2005, Gonzalez told Watt that Gonzalez had gained access to a computer system at fortunecity.com. Gonzalez then asked Watt for SSH exploit code to collect user names and passwords. ("Exploit code" is computer

programming designed to take advantage of a glitch or vulnerability in software running on a computer system.) Watt offered to write an SSHD runtime process infection (which would only operate in active memory and would thereby would avoid detection). Two weeks later, Watt informed Gonzalez that Watt's SSHD process injection exploit ("injectso") was finished, and transferred the exploit to Gonzalez along with a file named "INSTRUCTIONS."

The instant messenger logs reflect that in the days that followed, Watt and Gonzalez collaboratively attempted to deploy Watt's exploit on db2.fortunecity.com and securehq.bizrate.com; both attempts were unsuccessful despite having root (system administrator) privileges. However, Gonzalez and Watt were able to successfully deploy Watt's exploit on mozart.fiu.edu, part of the Florida International University network.

Watt Unquestionably Knew That Gonzalez Sold Vast Numbers of Credit and Debit Card Numbers Which He Stole Through Hacking Business Networks

Watt and Gonzalez discussed openly Gonzalez's sale of "dumps" (stolen credit and debit card numbers) and efforts to crack the DES encryption of the associated PIN numbers, as the following excerpt from a March 7th chat reflects.[1]

[1] For clarity, Gonzalez's alias "supreme team 04" and Watt's alias "MCCSucks2" have been replaced by their names. The text in brackets have been inserted for explanation and does not appear in the original.

[14:24] **GONZALEZ**: you have got to convince typedeaf to do some work for me, if he was able to hack some euro dumps we can make a fortune, I hacked a place and took ~30k [30,000] euro dumps [stolen credit/debit card numbers] and this last week I made ~11k [11,000] from only selling ~968 [approximately 968] dumps

[14:25] **WATT**: wow

[14:25] **GONZALEZ**: people want dumps from switzerland, france (best seller), spain, etc.,

[14:26] **GONZALEZ**: turkish too

[14:26] **WATT**: how did you get that place

[14:26] **WATT**: targetting

[14:26] **WATT**: or luck?

[14:27] **GONZALEZ**: pure luck

[14:27] **WATT**: heh

[14:27] **WATT**: keylogs? [secretly recorded logs of the keys struck by a computer user on his/her keyboard]

[14:27] **GONZALEZ**: yup

[14:27] **WATT**: jesus

[14:28] **WATT**: can u make me a list of sites that should be checked out?

[14:29] **GONZALEZ**: the russian thats working on the descracker shit [breaking the encryption on PIN numbers], he';s got access to a couple high profile tech sites where he specifically targets visitors based on their IP using 0day browser exploits [means of exploiting unknown or unpatched vulnerabilities in web browsers such as Internet Explorer], for example banks

Gonzalez Bragged Repeatedly to Watt About the Scope of the Fraudulent Scheme With Which Watt Was Assisting

The scope of what Gonzalez referred to in his discussions with Watt as "operation get rich or die tryin" continued to expand. As it did, Gonzalez repeatedly sent Watt links to news stories reflecting its impact. One of the articles sent to Watt, contained in PC World magazine, described a world wide wave of debit card fraud. The story pointed to one of Gonzalez's corporate victims, OfficeMax, as potentially being compromised and the source of the debit card with PIN information frauduently being used with increasing furor in several countries.

The vast scope of the operation in which Watt was participating with Gonzalez was not only readily apparent to him through the major press attention which was being drawn to his attention by Gonzalez, but also through the profits it was generating. Watt was one of the handful of intimate associates attending Gonzalez's $75,000 birthday party. In one conversation, Gonzalez lamented that he was trying to count more than $340,000 in cash manually because his money counter had just broken. The money was all in $20 bills, the denominations that would be obtained from ATMs with fraudulent debit cards. In a separate, contemporaneous exchange, Watt explored how much Gonzalez would be able to invest in a club he was considering opening. Gonzalez responded that it would depend on how they

would accept money from him; noting that he could probably get approximately $300,000 in a legitimate appearing form if someone needed a check, but most of his money was in cash.

The Sniffer Program Provided by Watt for Use By Gonzalez in Compromising TJX's Computer Network Was Specifically Tailored by Watt for the Purpose

Gonzalez, who remains Watt's intimate friend of a decade, has protectively stated that he did not tell Watt the purpose for which he needed the "sniffer" program so critical to the TJX data theft. While transparently supportive of his best friend, the notion of benign ignorance is squarely inconsistent with the facts. The two communicated constantly on all aspects of what they were doing on a daily basis. Watt did not simply take a "sniffer" program off of a virtual shelf and hand it to Gonzalez. The program was modified to specifically target those areas of the computers' network through which payment card numbers flowed on the TJX system. Further, as Gonzalez has also stated, when the "sniffer" program did not work at first, Watt modified it to ensure that it would.

Watt's apartment, too, was searched. The search took place late in the investigation, after he had meet Gonzalez several times in pretrial detention and knew his exposure as well. Nevertheless, in the same area where Watt stored his computer was a crumbled piece of paper containing an IP address (the address which identifies the location of a computer on the

Internet). That address was for the server to which the conspirators had transferred a large bulk of the debit and credit card numbers stolen from TJX.

Conclusion

Watt not only could foresee, but unquestionably knew, that he was collaborating with Gonzalez on breaking into business's computer networks to steal the massive numbers of credit and debit card numbers which they processed for sale and fraudulent use. Gonzalez explicitly told his good friend about what they were doing, the profits they were making and the press attention they were getting, as the vignettes above evidence.

Watt was not the group's leader, however. Indeed, the statements of coconspirator Patrick Toey and the instant messaging logs reflect that Gonzalez was sometimes irritated by the time it took for Watt to do some of the coding Gonzalez wanted.

The advisory guideline sentencing range of mandatory life was inappropriate here, in light of the extent and nature of Watt's involvement in the broader series of massive identity thefts perpetrated by the group nationwide. However, that does not mean that it should be disregarded.

Watt has argued that even were a substantial loss reasonably foreseeable to him from the course of his collaboration with Gonzalez, the extent of the loss caused to TJX, which has a major

impact on the Guidelines calculations, was not. Even, as a second point of guidance, cabining the harm readily foreseeable to Watt merely to what Gonzalez explicitly described to him in the first week of March, 2005, Watt's advisory Guidelines range would be 11-15 years' imprisonment, at a minimum.

For these reasons, the court should impose a sentence of five years imprisonment, followed by a three year period of supervised release on Steven Watt at the time of sentencing.

Respectfully submitted,

MICHAEL K. LOUCKS
Acting United States Attorney

By: */s/Stephen P. Heymann*
Stephen P. Heymann
Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann
Stephen P. Heymann
Assistant U.S. Attorney

Date: June 1, 2009